

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for controlling access to protected resources within a distributed data processing system, the method comprising:
 - receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;
 - validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;
 - determining that the single-use token is a domain token;
 - generating a client authorization credential request;
 - sending to a second server the client authorization credential request, the single-use domain token associated with the client or the use of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain;
 - generating a response to the request;
 - refreshing the single-use token;
 - validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server;
 - generating the client authorization credential; refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server; and
 - sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server; and
 - sending the response and the refreshed single-use token to the client.
2. (Currently Amended) The method of claim 1 further comprising:
 - receiving the single-use service token, wherein the single-use service token is issued by the first server; and
 - refreshing the single-use service token at the first server.

3. (Original) The method of claim 1 wherein the session information in the single-use token is a session key.

4-5. (Canceled)

6. (Currently Amended) The method of claim [[5]] ~~1~~ further comprising:
storing the client authorization credential at the first server;
generating a single-use service token associated with the client or the user of the client;
and
sending to the client the single-use service token along with the response and the single-use domain token.

7. (Original) The method of claim 1 further comprising:
receiving a login request from the client at the second server;
challenging the client to provide authentication data; receiving authentication data from the client;
authenticating the client;
generating a single-use domain token associated with the client or the user of the client;
generating an authentication response; and
sending the authentication response and the single-use domain token to the client.

8. (Original) The method of claim 7 further comprising:
determining that the login request is a redirected request from the first server; and
modifying the authentication response to redirect the client to the first server.

9. (Currently Amended) An apparatus for controlling access to protected resources within a distributed data processing system, the apparatus comprising:

~~means for~~ processing logic receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

~~means for~~ processing logic validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

~~means for processing logic~~ determining that the single-use token is a domain token;
~~means for processing logic~~ generating a client authorization credential request;
~~means for processing logic~~ sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain;
~~means for processing logic~~ generating a response to the request;
~~means for processing logic~~ refreshing the single-use token;
validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server;
generating the client authorization credential;
means for refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server; and
sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server; and
~~means for processing logic~~ sending the response and the refreshed single-use token to the client.

10. (Currently Amended) The apparatus of claim 9 further comprising:

~~means for processing logic~~ receiving a single-use service token, wherein the single-use service token is issued by the first server; and
~~means for processing logic~~ refreshing the single-use service token at the first server.

11. (Original) The apparatus of claim 9 wherein the session information in the single-use token is a session key.

12-13. (Canceled)

14. (Currently Amended) The apparatus of claim [[13]] 9 further comprising:

~~means for processing logic~~ storing the client authorization credential at the first server;

~~means for processing logic~~ generating a single-use service token associated with the client or the user of the client; and

~~means for processing logic~~ sending to the client the single-use service token along with the response and the single-use domain token.

15. (Currently Amended) The apparatus of claim 9 further comprising:

~~means for processing logic~~ receiving a login request from the client at the second server;

~~means for processing logic~~ challenging the client to provide authentication data; means for receiving authentication data from the client;

~~means for processing logic~~ authenticating the client;

~~means for processing logic~~ generating a single-use domain token associated with the client or the user of the client;

~~means for processing logic~~ generating an authentication response; and

~~means for processing logic~~ sending the authentication response and the single-use domain token to the client.

16. (Currently Amended) The apparatus of claim 15 further comprising:

~~means for processing logic~~ determining that the login request is a redirected request from the first server; and

~~means for processing logic~~ modifying the authentication response to redirect the client to the first server.

17. (Currently Amended) A computer program product on a non-transitory computer readable medium for controlling access to protected resources within a distributed data processing system, the computer program product comprising executable instructions configured for:

~~instructions for~~ receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

~~instructions for~~ validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

~~instructions for~~ determining that the single-use token is a domain token;

~~instructions for~~ sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain;
~~instructions for~~ generating a response to the request;
~~instructions for~~ refreshing the single-use token;
validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server;
generating the client authorization credential;
refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server; and
sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server; and
~~instructions for~~ sending the response and the refreshed single-use token to the client.

18. (Currently Amended) The computer program product of claim 17, said instructions further comprising configured for:
~~instructions for~~ receiving a single-use service token is a service token, wherein the single-use service token is issued by the first server; and
~~instructions for~~ refreshing the single-use service token at the first server.

19. (Original) The computer program product of claim 17 wherein the session information in the single-use token is a session key.

20-21. (Canceled)

22. (Currently Amended) The computer program product of claim 21 17, said instructions further comprising configured for:
~~instructions for~~ storing the client authorization credential at the first server;

~~instructions for~~ generating a single-use service token associated with the client or the user of the client; and
~~instructions for~~ sending to the client the single-use service token along with the response and the single-use domain token.

23. (Currently Amended) The computer program product of claim 17, said
instructions further comprising configured for:

~~instructions for~~ receiving a login request from the client at the second server;
~~instructions for~~ challenging the client to provide authentication data;
~~instructions for~~ receiving authentication data from the client;
~~instructions for~~ authenticating the client;
~~instructions for~~ generating a single-use domain token associated with the client or the user of the client;
~~instructions for~~ generating an authentication response; and
~~instructions for~~ sending the authentication response and the single-use domain token to the client.

24. (Currently Amended) The computer program product of claim 23, said
instructions further comprising configured for:

~~instructions for~~ determining that the login request is a redirected request from the first server; and
~~instructions for~~ modifying the authentication response to redirect the client to the first server.